دانشگاه صنعتی شریف

دانشکده مهندسی برق

آزمایشگاه پیشرفته برنامه‌نویسی

"شبکه و Socket Programming"

نیم‌سال دوم (بهار) ۰۰-۰۱

آزمایش هفتم

مقدمه

در این آزمایش می‌خواهیم از شبکه استفاده کنیم و اتصالی بین دو کلاینت برقرار کنیم. یکی از راه‌های انجام این کار استفاده از socket برای برقراری این اتصال است. ارتباط بین سوکت‌ها از طریق پورت‌ها صورت می‌پذیرد. برای کسب اطلاعات بیشتر درباره‌ی سوکت شبکه و پورت می‌توانید لینک‌های زیر را مطالعه کنید:

https://en.wikipedia.org/wiki/Network_socket

https://en.wikipedia.org/wiki/Port_(computer_networking)

در این آزمایش از دو نوع سوکت java.net.ServerSocket برای گوش دادن روی یک پورت و انتظار برای درخواست برقراری ارتباط از سوی برنامه دیگر و از java.net.Socket برای برقراری ارتباط استفاده می‌کنیم.

برنامه چت

می‌خواهیم برنامه‌ای بنویسیم که بتواند ارتباط متنی بین دو شخص که روی دو کامپیوتر مجزا هستند برقرار کند. برنامه دو نسخه‌ی server و client دارد.

راهنمایی: سرور برای هر کلاینتی که به آن متصل می‌شود باید thread جدیدی ایجاد کند در غیر این صورت نمی‌تواند هم زمان به درخواست‌ها و ارسال‌های همه کلاینت‌ها گوش دهد.

ابتدا باید برنامه سرور را run کنید. کاربران از طریق برنامه client با سرور ارتباط برقرار خواهند کرد. هر شخص یک username برای خود انتخاب می‌کند. این username به server فرستاده می‌شود و در صورتی که قبلا چنین اسمی در سرور ثبت نشده بود، از کاربر رمز عبور او را پرسیده و ثبت نام شخص پذیرفته می‌شود. (در غیر این صورت شخص باید username دیگری انتخاب کند.)

امتیازی(20 نمره): در اینترنت در خصوص ملزومات رمز عبور قوی سرچ کرده، آن را به کاربر اطلاع داده و تنها رمز عبوری را بپذیرید که حداقل‌های ذکر شده را داشته باشد.

امتیازی(30 نمره): برای انتقال و ذخیره رمز عبور کاربرها در سرور راهکاری امنیتی پیشنهاد کرده و آن را پیاده کنید.

راهنمایی: می‌توانید از هش استفاده کرده و به جای آن که رمز عبور را به صورت Plain-text منتقل، ذخیره و بررسی کنید، با هش آن کار کنید. واضح است در این حالت برای چک کردن ملزومات رمز عبور، نمیتوانید از روی رمز عبور هش شده متوجه قدرت و بعدا در فرایند Login متوجه صحت آن شوید. بدین منظور

راهکاری ارائه دهید که کاربر نتواند این سازوکار چک کردن قدرت رمز عبور را Bypass کند و در سرور نیز بررسی رمز عبور بدون رمزگشایی آن صورت گیرد.

پس از اینکه ثبت نام با موفقیت انجام شد، شخص می‌تواند درخواست برقراری ارتباط با دیگران را بدهد. بدین منظور باید بتواند لیست تمامی کاربران را مشاهده کند و username مخاطب خود را به سرور ارسال کند. درصورتی که مخاطب online باشد، سرور تقاضای برقراری ارتباط را به او منتقل می کند. اگر مخاطب تقاضا را بپذیرد، سرور به هر دو طرف اطلاع می‌دهد که می‌توانند گپ زدن را شروع کنند.

امتیازی(20 نمره): در بخش مشاهده کاربران، قابلیت فیلتر کردن کاربران براساس آنلاین یا آفلاین بودن را اضافه کنید.

از این به بعد نوشته‌های دو شخص برای همدیگر ارسال می‌شود. توجه شود که دو شخص هیچ ارتباط مستقیمی با یکدیگر ندارند و همه چیز از طریق سرور دریافت و ارسال می‌شود.

توجه: برنامه شما باید اورهای مختلف را به دسترسی شناسایی و هندل کند؛ برای مثال عدم وجود نام کاربری درخواست شده، قطع شدن یکی از کاربران و .. را به دسترسی کنترل کرده و پیام خطای متناسب را به کاربر نشان دهد.

امتیازی(30 نمره): در بخش چت کردن دو کاربر قابلیت کد کردن Base64 را اضافه کرده تا کاربران در صورت تمایل بتوانند محتوای پیام خود را کد کنند. همچنین این قابلیت را اضافه کرده که سرور متوجه پیام‌های کد شده با Base64 شده و در صورت صلاحدید کاربر مدیر سرور، آن‌ها را Decode کرده و به مدیر نشان دهد.

امتیازی(60 نمره): در بخش چت کردن دو کاربر قابلیت رمزنگاری نامتقارن را اضافه کرده تا کاربران در صورت تمایل بتوانند با تبادل یک کلید بین یکدیگر، محتوای پیام خود را رمز کرده و از دید سرور مخفی کنند.

امتیازی:(20 نمره): در سرور این قابلیت را اضافه کرده که انتقال کلید رمزنگاری نامتقارن را تشخیص داده و در صورت صلاحدید کاربر مدیر ، جلوی این انتقال را گرفته و کاربران خاطی را از سیستم اخراج کند.